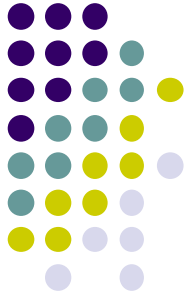
Quantum Computing



Bartolomeo Montrucchio

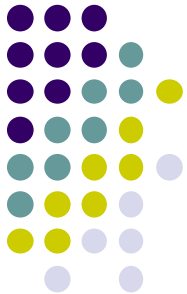
Politecnico di Torino

Dipartimento di Automatica e Informatica (DAUIN)

Torino - Italy

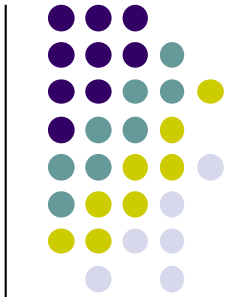
bartolomeo.montrucchio@polito.it

Introduction



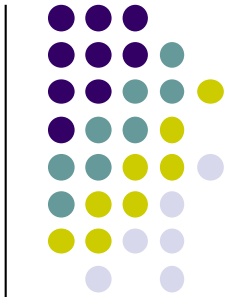
- Quantum computing could be really important in:
  - industries where are significant optimization problems
  - pharmaceuticals and drug discovery
  - new materials, like high temperature superconductors
  - secure information communications and cybersecurity
  - financial services
  - artificial intelligence
- We want a Universal fault-tolerant quantum computer (QC)
  - now there is an approximate quantum computer
  - there are also quantum annealed based QCs

Introduction



- When Quantum Computers will be available
  - in a few years?
  - in a couple of decades?
  - never [Dyakonov19]?
- Error rate must be lowered
- Coherency time must be improved (now some tens of μs)
- Topology is important
  - Qubits optimal for the selected algorithm should be found by means of a compiler
- QCs are now coprocessors
- Quantum Advantage [Monroe19]
- Quantum Supremacy
  - solving selected problems faster than a conventional computer

Classical computers

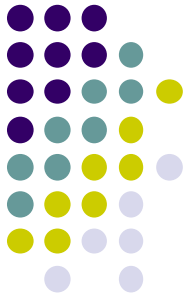


- Physical model
  - mechanical (Babbage)
  - electrical
  - optical
  - biological (e.g a person)
- Conceptual model
  - Von Neumann architecture
  - Turing machine
  - Cellular automata (e.g. Game of Life)

History of QC

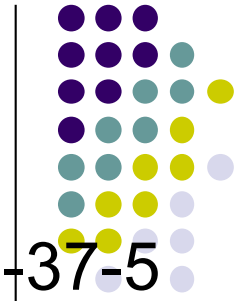
- Richard P. Feynman(International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, pp. 467-488, 1982)
  - ”how can we simulate the quantum mechanics?...Let the computer itself be built of quantum mechanical elements which obey quantum mechanical laws”
  - “Can a quantum system be probabilistically simulated by a classical (probabilistic, I’d assume) universal computer?....No!”
- Shor’s algorithm
  - factorization of large numbers
- Quantum error correcting codes
  - to enable QCs to operate also in presence of errors
- QCs are able to solve some problems more efficiently than possible with classical computer, even is classical is strongly improved [Monroe19]
  - QCs can not be emulated from a conventional computer
  - even if PH(polynomial hierarchy)=NP(non polynomial time)=P(polynomial time), BQP(Bounded Quantum Polynomial) would still be separate

Introduction to Quantum Mechanics



- Interference experiment with bullet ([Feynman64 I-37-3])
- Interference experiment with water waves ([Feynman64 I-37-3])
- Interference experiment with electrons ([Feynman64 I-37-5])
  - superposition of probability amplitudes
- Interference experiment with electrons while “watching” them ([Feynman64 I-37-7])
- Quantum mechanics with bullets? ([Feynman64 I-37-10])
- Binary amplitude grating (see video)
- Sinusoidal amplitude grating (see video)

Introduction to Quantum Mechanics



- Interference experiment with electrons ([Feynman64 I-37-5 III-3-2])
  - superposition of probability amplitudes
- The probability that a particle starting from the electron gun s will arrive at the detector x is the absolute square of a complex number called a probability amplitude
- This amplitude is represented with Dirac notation, where ⟨ ⟩ are equivalent to "the amplitude that"

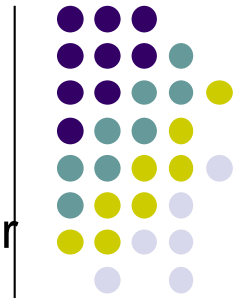
⟨particle arrives at x | particle leaves s⟩

final condition is at the left of | starting condition is at the right of the |

it can be written as ⟨x|s⟩ pronounced bra x ket s ➔ bracket notation

"THE AMPLITUDE THAT A PARTICLE FROM S WILL ARRIVE AT X"

Postulates of Quantum Mechanics [Nielsen00 p.80]



1: any isolated physical system is completely described by its state vector
- simplest quantum mechanical system is the qubit; has a two-dimensional state space
- given |0> and |1> an orthonormal basis of the space
- state vector is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$
  where $|\psi\rangle$ is a unit vector, $\langle\psi|\psi\rangle=1$
  equivalent to $|\alpha^2|+|\beta^2|=1$ (normalization condition)

2: the evolution of a closed quantum system is described by a unitary transformation U, that is $|\psi'\rangle = U|\psi\rangle$
example of U is the Hadamard operator
If we apply U, this means there is a we who is outside the closed system, therefore the system is not completely closed; this produces noise; since we need to apply U (for programming the computer) we need to control noise
(unitary => reversible, but reversible is not unitary for sure)
(please note that a reversible computing system would not expend energy at all, since it does not erase information [Nielsen00 p.153])

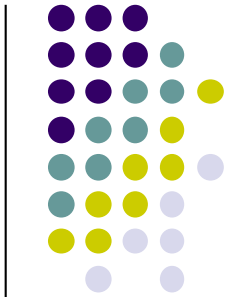
Postulates 3 (observation in quantum mechanics is an invasive procedure) and 4 (entanglement) omitted ([Nielsen00 p.84 and p.94]

Introduction to Quantum Mechanics

- Polarization of one photon ([Feynman64 III-11-10])
- Let's suppose a photon is polarized along x' by a piece of Polaroid; any state can be represented as a linear combination of the two base states $|x\rangle$ and $|y\rangle$
  - $|x'\rangle = \cos \vartheta \, |x\rangle + \sin \vartheta \, |y\rangle$
- Which is the probability that the photon passes through a further Polaroid along x (ϑ=0)?
  - $\langle x|x'\rangle = \cos \vartheta \, \langle x|x\rangle + \sin \vartheta \, \langle x|y\rangle$
  - since $\langle x|y\rangle$=0 and $\langle x|x\rangle$=1,
    - $\langle x|x'\rangle = \cos \vartheta$ ➔ the probability is $\cos^2 \vartheta$ (absolute square of the complex number)

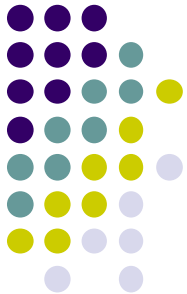
classically the energy is $\cos^2 \vartheta$ weaker

Qubit



- a qubit q is the quantum version of a bit
  - again in base 2
  - built with two-state systems (there exist N state systems also)
    - 3-level quantum system is called a qutrit (like a trit, base 3 bit)
    - d-level quantum system is called qudit
- quantum state of Qubit can take values of |0>, |1>, or **both at once (superposition)**
  - |0> and |1> (ket 0 and ket 1) are called the standard (or computational) basis, and <0|1> = 0
- q= $\alpha|0\rangle + \beta|1\rangle$ [Nielsen00]
  - where α and β (α and β are amplitudes [Nielsen00 p.81]) are complex numbers while $|\alpha|^2+|\beta|^2=1$ ($|\alpha|^2$ is a probability [Nielsen00 p.13])
- measuring a qubit means to project it (collapsing in one of the two states), with a probability of $|\alpha|^2$ to be 0 and of $|\beta|^2$ to be 1
- collapsing is very useful for computer security!

Qubit registers



- a qubit register of 2 qubits is:
  - qr= a|00⟩ + b|01⟩ c|10⟩ + d|11⟩
- Let's suppose having:
  - ß=w|00⟩ + w|11⟩
- if we measure the second qubit of ß and it appears to be 1
  - the first WILL BE 1 => entanglement
- useful for teleportation (no Star Trek, unfortunately)

Bloch sphere (I)

- Bloch sphere can represent 1 qubit only (2 complex numbers, but probability must sum => 3 values)
- |0> and |1> are on the North Pole and on the South Pole and are orthogonal each other

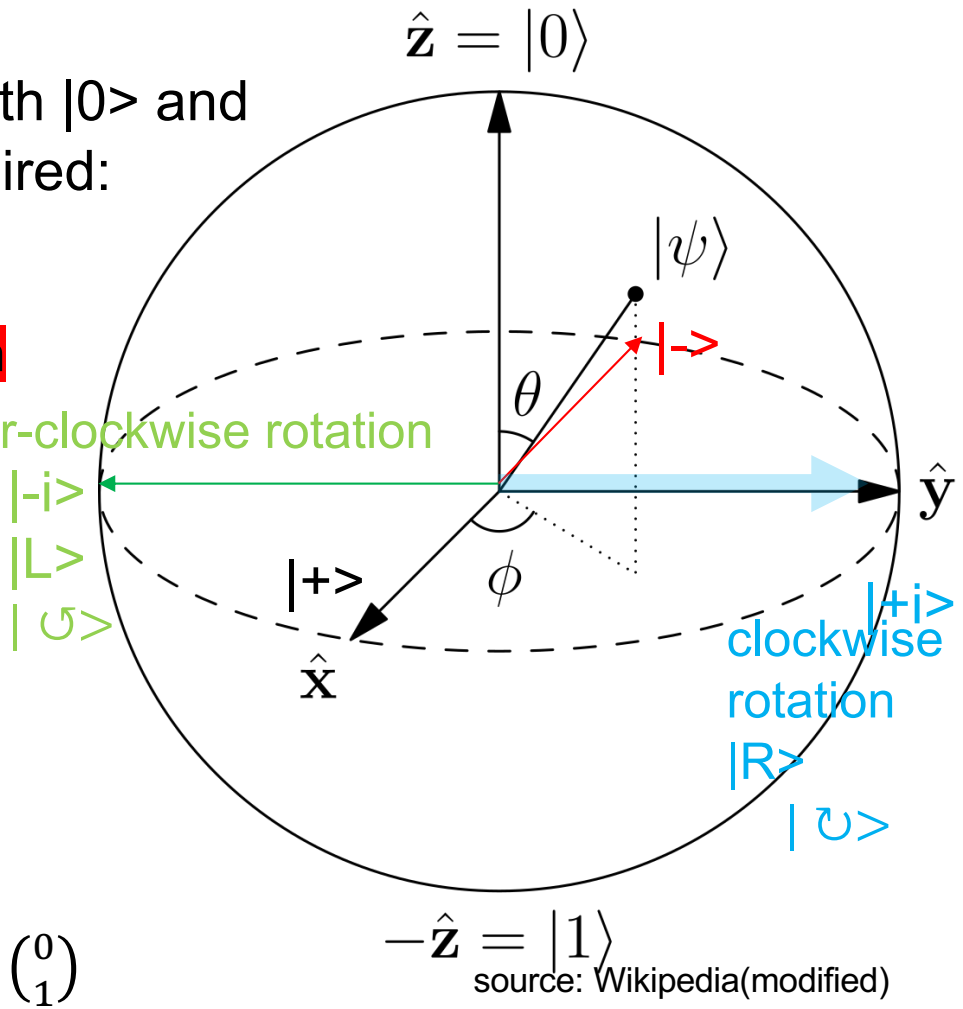
- ATTENTION: on the Bloch sphere North |0> and South |1> are NOT orthogonal as required:
  - BECAUSE they are orthogonal in the Hilbert space => means that a system cannot be both spin-up and spin-down
- changing θ (e.g. starting from |0>) produces a superposition of |0> and |1>
- changing ϕ means changing the phase of the qubit (gate Z, S and T)

$$|\psi> = \alpha|0> + \beta|1> = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$|\alpha^2| + |\beta^2| = 1$$

$\alpha = \cos(\theta/2)$ // real value

$\beta = e^{i\phi}\sin(\theta/2)$ // phase e.g. $|1> = \begin{pmatrix}0\\ 1\end{pmatrix}$



source: Wikipedia(modified)

Bloch sphere (II)

$$|\psi>=\begin{pmatrix}\cos\frac{\theta}{2}\\ e^{i\phi}\sin\frac{\theta}{2}\end{pmatrix} \qquad \begin{cases}x=\sin\theta\cos\phi\\ y=\sin\theta\sin\phi\\ z=\cos\theta\end{cases}$$

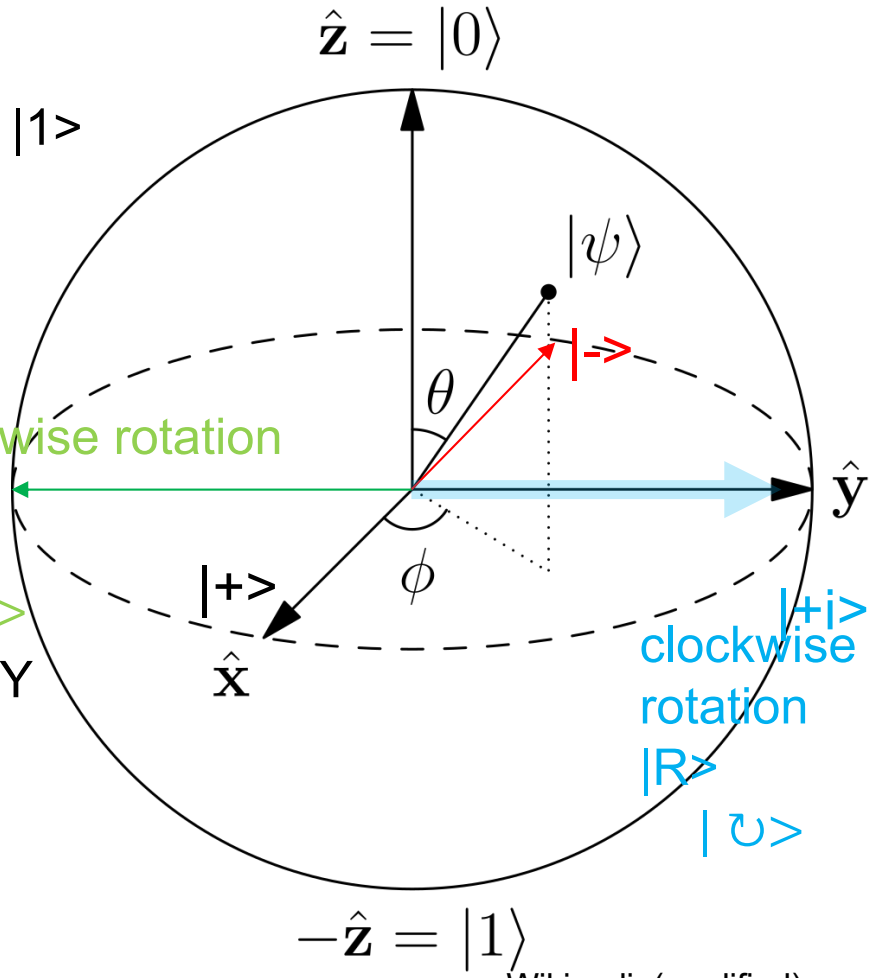
Basis:

- Computational (standard or Z basis) |0> and |1>
- Plus and minus basis (diagonal or X basis)

$$|+>=\frac{|0>+|1>}{\sqrt{2}} \qquad |->=\frac{|0>-|1>}{\sqrt{2}}$$

- Clockwise and counterclockwise (circular or Y basis)

$$|\circlearrowright>=\frac{|0>+i|1>}{\sqrt{2}} \qquad |\circlearrowleft>=\frac{|0>-i|1>}{\sqrt{2}}$$



source: Wikipedia(modified)

Quantum gates (I)

- *X* gate, which is known as a “bit-flip” (flips |0> to |1> and vice versa); it is similar to a classical NOT gate
- *H* (Hadamard) gate is a rotation around the X+Z axis
  - starting from |0> a perfect superposition (50%-50% of |0> and |1>) is produced
  - applying again H, |0> is obtained again (deterministic)
  - but H-Z-H changes the phase (amplitude or better probability amplitude) without changing probability => see Grover’s algorithm (uses Controlled-Z)

- Doing H-T-H there is no more 50%-50% because the second H starts from a point on the plane X-Y that is not |+> and after π rotation around X+Z axis the final point is with $0<\theta<\pi/2$ => superposition

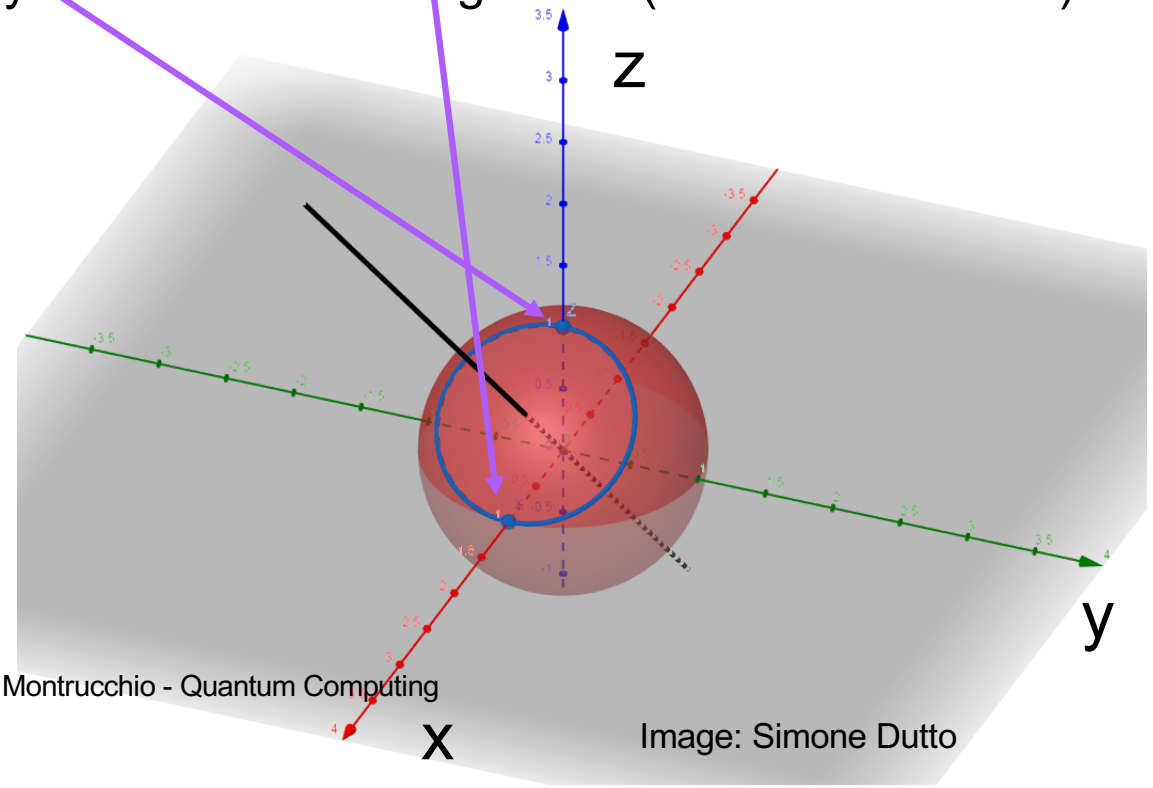
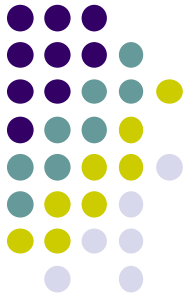


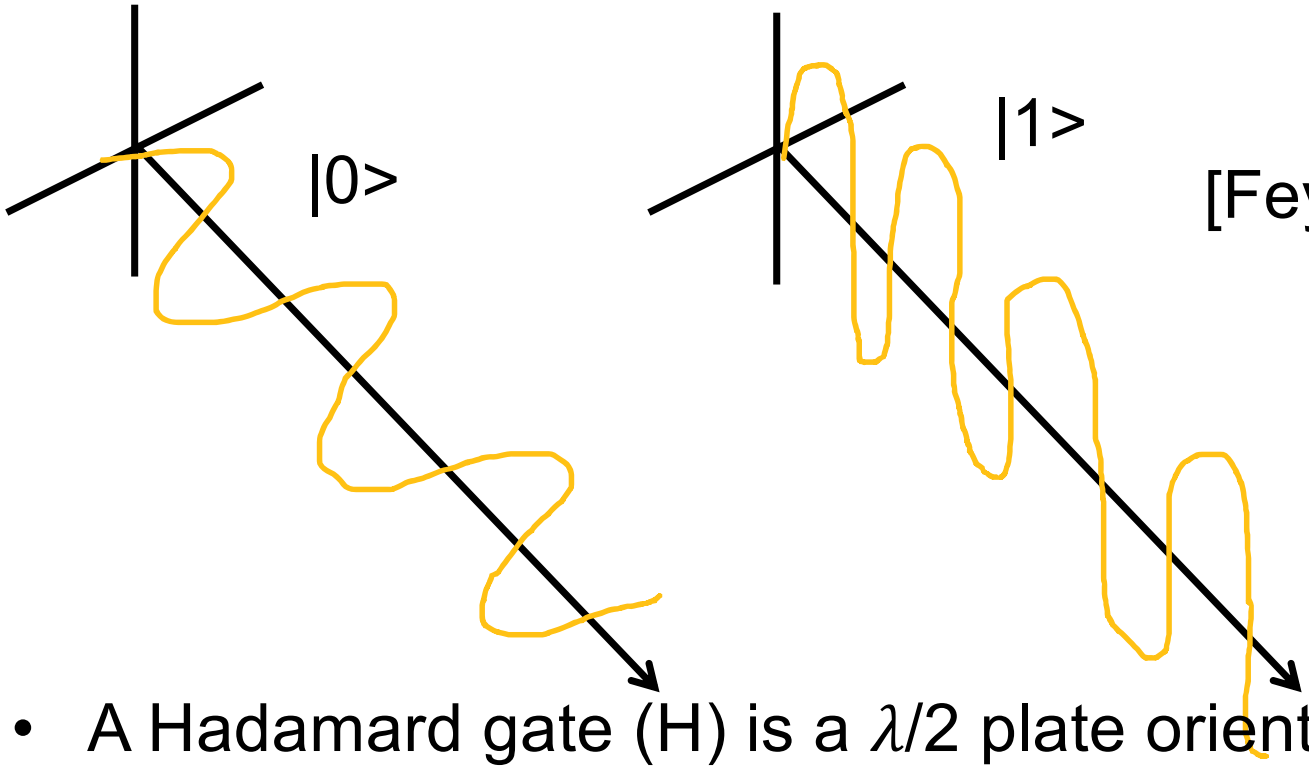
Image: Simone Dutto

Quantum gates (II)



- *Z* gate is a *π* rotation around the Z axis
  - phase-flip
- *S* gate is a rotation of *π*/2 around *Z*
- *T* gate is a *π*/4 rotation around *Z*
- *S*† is the inverse of *S* (does a −*π*/2 around Z)
- *T*† is the inverse of *T (does a -π*/4 rotation around Z)
- Y is a combined bit-flip (X) and phase-flip(Z)
  - X+Z

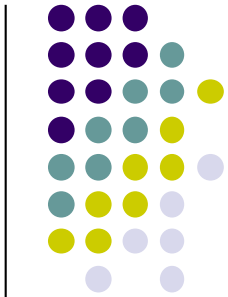
Qubit with a photon



[Feynman64 III-11-10]

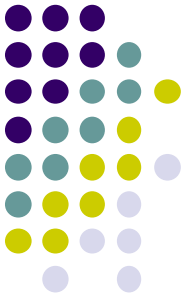
- A Hadamard gate (H) is a $\lambda/2$ plate oriented at 22.5°
- A general gate is an arbitrary rotation by means of a $\lambda/4$-$\lambda/2$-$\lambda/4$ sequence of wave plates
- Right circular polarization is |+i>
- Left circular polarization is |-i>

Quantum gates (III)



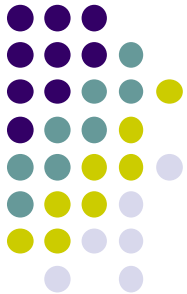
- CNOT is the controlled NOT
  - it is a quantum EXOR, that is a reversible EXOR
    - |A,B> → |A,B⊕A> where ⊕ is an addition modulo 2 (the EXOR gate) [Nielsen00 p.21]
  - the controlled value (with the EXOR symbol) is negated if the controller is 1, otherwise it remains equal
  - doing H-CNOT(with H on the controller) on |00>
    - after H result is (|00>+|10>)/$\sqrt{2}$
    - after H-CNOT (with H on the controller), CNOT flips the second qubit if the first is excited => (|00>+|11>)/$\sqrt{2}$ ➔ ENTANGLEMENT ([Corbett19] p.73)
  - controller and controlled values positions depend also from the hardware architecture of the QC qubits
    - In IBM Q custom topology CNOT can be put everywhere
    - In IBM Q actual computers, CNOT controller and controlled positions depends on the qubits topology (directed graph)

Quantum gates (IV)



- Controlled-Z
  - like CNOT produces a X (that is a NOT) if controller is 1, Controlled-Z produces a Z only if the controller is 1
  - Doing H-ControlledZ-H the phase is reversed under control (see Grover)
- Toffoli
  - it is a universal gate for reversible computation
  - similar to NAND used in classical computation

Quantum gates (V)



- In IBM computer gates:
  - u1(λ)=U(0,0,λ), u2(φ, λ)=U(π/2,φ,λ) and u3(θ,φ,λ)=U(θ,φ,λ)
  - e.g. H=u2(0,π)

allow $|\psi\rangle$ = U $|\psi\rangle$, where:

$$U = \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} & e^{i\lambda+i\varphi}\cos\frac{\theta}{2} \end{pmatrix}$$

Examples

- $|0> \xrightarrow{X} |1> \xrightarrow{H} \frac{1}{\sqrt{2}}(|0> - |1>) \xrightarrow{X} \frac{1}{\sqrt{2}}(|1> - |0>)$
  $\xrightarrow{H} \frac{1}{2}(|0> - |1> - |0> - |1>) = -|1>$
  - amplitude changes its sign
- $|0> \xrightarrow{H} \frac{1}{\sqrt{2}}(|0> + |1>) \xrightarrow{X} \frac{1}{\sqrt{2}}(|1> + |0>) \xrightarrow{H} |0>$
  - amplitude does NOT change sign

QC Computers and Simulators

- It is possible to run actual QC programs or simulate quantum circuits (and Bloch sphere)
  - [IBMQ] Graphical interface and Python based emulator and OpenQASM system
    - cloud usage of the true QC computer possible
  - [D-Wave] Quantum annealing based (5000 qubits July 2020) computer
    - cloud usage of the true QC computer possible
  - [MS18] Q# language (emulator)
  - [Rigetti18] development kit
  - [Corbett19] software for IBM Q
  - [QCsim19] with a list of simulators (in particular Quirk)

IBM Q Quantum Composer and languages

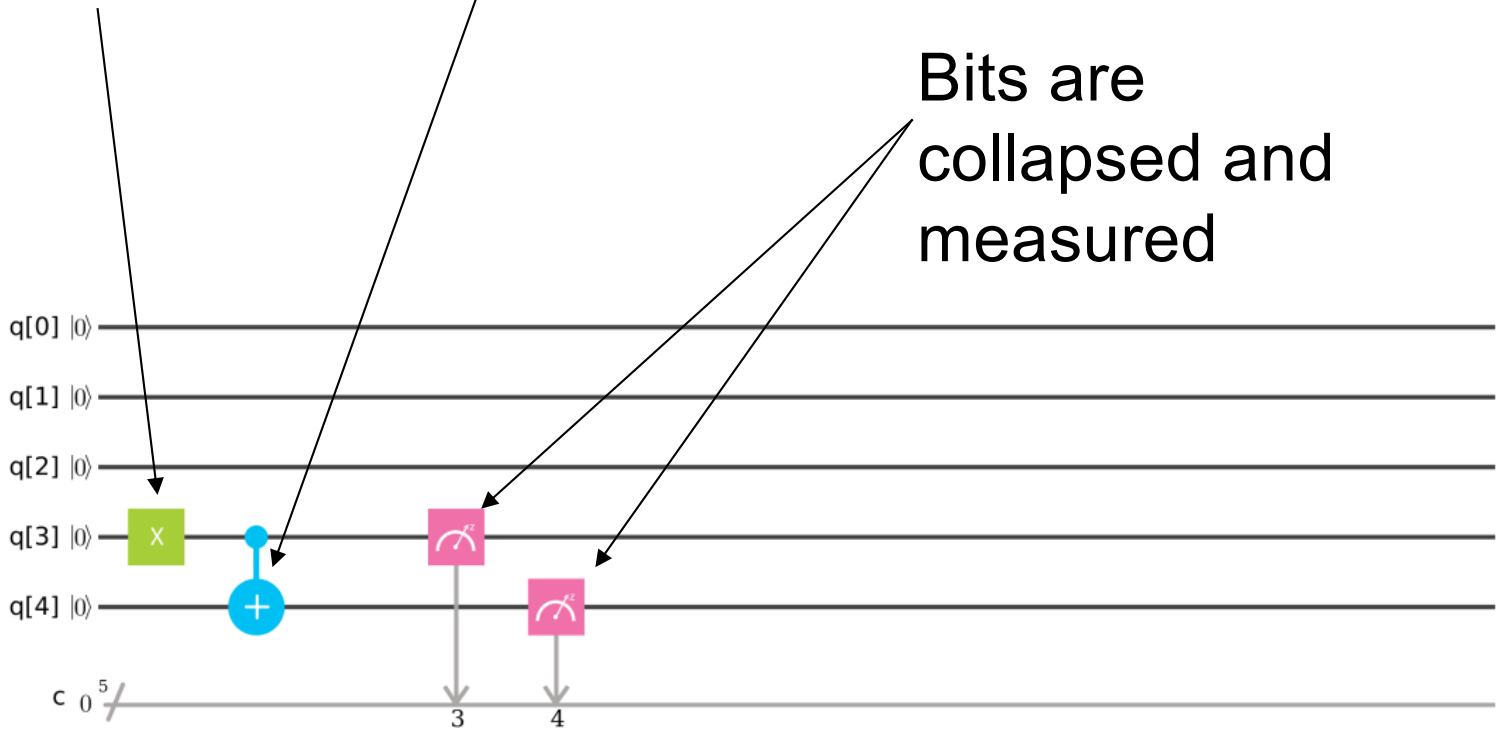
- Quantum Composer is similar to a musical score [Corbett19]
  - each line is a qubit
  - time flows from left to right
- There are 3 possibilities:
  1. Real Quantum Processor => in Simulation
  2. Real Quantum Processor => in Running
  3. Custom Topology (ALL to ALL qubits, max 20) => in Simulation only!
- There is also the possibility of having OpenQASM language version
- Third possibility is QISKit
  - Python based

IBM Q example

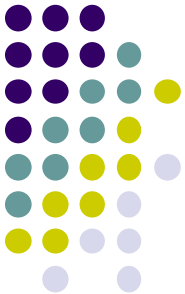
|0> is inverted by X gate and becomes |1>

CNOT gate: q[4] is inverted (NOT) if q[3] is 1, otherwise q[4] is unaltered

Bits are collapsed and measured

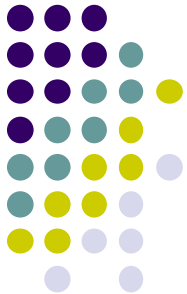


Entanglement and teleportation



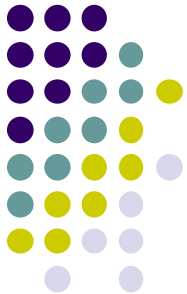
- Using CNOT it is possible to produce entanglement between two bits
- It is then possible to separate the two qubits (at speed lower than c !)
- Finally collapsing one qubit (50% of 1 and 50% of 0)
  - the other qubit will be entangled as soon as it will be collapsed also
  - no matter distance

Classical and Quantum complexity



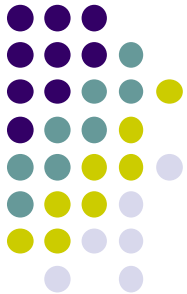
- if superposition is not used, QC is like a classical computer [LaUh09 p.23]
- in terms of computability, classical and quantum computers are almost equivalent
- factorization of a n-bit integer is a NP problem (non polinomial, in particular exponential for a classical computer)
  - it is polinomial on a QC with Shor's algorithm
- however this improvement is not sure for all NP problems

Advantages and disadvantages of QC



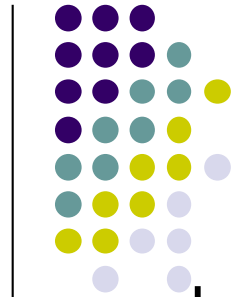
- Entire known universe could be put in 2^{800} bits of information
  - The entire universe could be simulated in parallel with 800 qubits? NO
  - Inizialization would require 2^{800} operations, too slow
  - Output would require 2^{800} steps, or in the best case 2^{400}
- Quantum information can not be forged and the destructive nature of measurements means we can find eavesdroppers
  - great for computer security applications!

Amplitude amplification



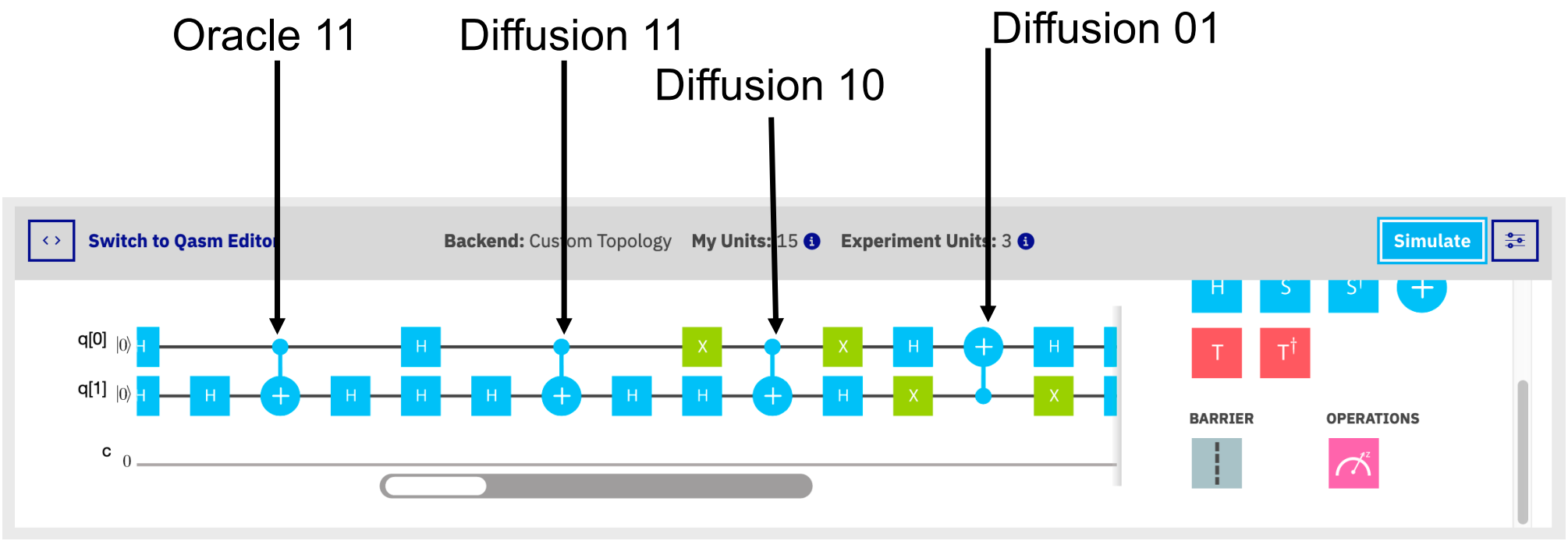
- A standard register of n bits can have $N=2^n$ states, but only one at a time
- An n qubits register has in the same time $N=2^n$ values
  - when I read it, it collapses in one of the 2^n states
- It is possible:
  - to create a uniform superposition (with Hadamard)
  - to modify the probability distribution increasing the probability of the solution we want
  - to measure the system (collapsing it) and get the result
  - more than one full iteration is required (it is probabilistic)

Grover (I)

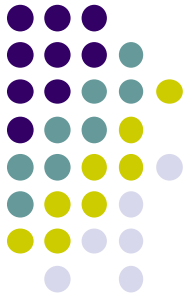


- With Grover's algorithm [LaUh09 p. 39] it is possible to search:
  - in an unstructured an unsorted database with N elements
  - classical complexity is O(N)
    - sequential search (binary search O(log(N)) while hash table O(1), but data are ordered)
- $O(N^{1/2})$ is sufficient with the QC
- Using more or less than $O(N^{1/2})$ reduces the probability of success
  - E.g. with n=3 qubits, $2^n = 8$ elements in the search space, after:
    - 0 iteration with a uniform superposition ➔ probability of success is about 0.125
    - 1 iteration with a uniform superposition ➔ probability of success is about 0.78
    - 2 iteration with a uniform superposition ➔ probability of success is about 0.95
    - 3 iteration with a uniform superposition ➔ probability of success is about 0.33
- See https://www.youtube.com/watch?v=Uw6zEMSxKvg

Grover (II)

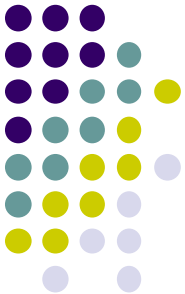

Oracle 11
Diffusion 11
Diffusion 10
Diffusion 01
Switch to Qasm Editor
Backend: Custom Topology
My Units: 15
Experiment Units: 3
Simulate
q[0]
q[1]
c
BARRIER
OPERATIONS

Bibliography (I)



- [Feynman64] Richard P. Feynman, Robert B. Leighton, Matthew Sands, “The Feynman Lectures on Physics”, Volume III: Quantum Mechanics, http://www.feynmanlectures.caltech.edu
- [Glas01] Andrew Glassner, “Quantum Computing”, IEEE Computer Graphics and Applications, July-Sept, Nov 2001, https://www.glassner.com/wp-content/uploads/2014/04/CG-CGA-PDF-01-07-Quantum-Computing-1-July01.pdf https://www.glassner.com/wp-content/uploads/2014/04/CG-CGA-PDF-01-09-Quantum-Computing-2-Sept01.pdf https://www.glassner.com/wp-content/uploads/2014/04/CG-CGA-PDF-01-11-Quantum-Computing-3-Nov01.pdf
- [LaUh09] Marco Lanzagorta, Jeffrey Uhlmann, “Quantum Computer Science”, Morgan&Claypool, 2009, ISBN 9781598297324 https://www.amazon.it/Quantum-computer-Science-Marco-Lanzagorta/dp/1598297325/ref=sr_1_1?ie=UTF8&qid=1546799228&sr=8-1&keywords=quantum+computer+science+lanzagorta
- [Nielsen00] Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge, 2000

Bibliography (II)



- [IBMQ] IBM Q Experience https://quantumexperience.ng.bluemix.net/qx/experience
- [D-Wave] D-Wave systems, https://www.dwavesys.com/quantum-computing
- [MS18] Microsoft Q# https://docs.microsoft.com/en-us/quantum/?view=qsharp-preview
- [Rigetti18] Dave Yen, How to write a quantum program in 10 lines of code, https://medium.com/rigetti/how-to-write-a-quantum-program-in-10-lines-of-code-for-beginners-540224ac6b45
- [Corbett19] Christine Corbett Moran, Mastering Quantum Computing with IBM QX, Packt Publishing Ltd, 2019, ISBN 978-1-78913-643-2
- [QCsim19] https://www.quantiki.org/wiki/list-qc-simulators

Bibliography (III)

- [Eco17] Jason Palmer, “Here, There and Everywhere. Quantum Technology Is Beginning to Come into Its Own,” Economist, March 9, 2017 https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own
- [Tang18] Ewin Tang , A quantum-inspired classical algorithm for recommendation systems https://arxiv.org/abs/1807.04271
- [Tts1806] Luigi Grassia, “INVESTIMENTO MILIARDARIO FORMERÀ I SUPER-INGEGNERI - Cervelli cercansi - Mega-progetto Usa per vincere la corsa ai computer quantistici”, Tuttoscienze n.1806, 19 settembre 2018, LaStampa p.29
- [Dyakonov19] Mikhail Dyakonov, “The Case Against QUANTUM COMPUTING”, IEEE Spectrum, Mar 2019, pp.25-29
- [Monroe19] Don Monroe, “Quantum Leap”, Communications of the ACM, Jan 2019, pp.10-12